2131
#5
8-29-03
AM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 074273/0163

Applicant: Satoshi OBANA

Title: ENCRYPTION AND DECRYPTION WITH ENDURANCE TO CRYPTANALYSIS METHOD

Serial No.: 09/553,415

Filed: April 20, 2000

Examiner: Unassigned

Art Unit: 2766

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §1.56 and 37 CFR §1.97

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Submitted herewith on Form PTO SB/08 is a listing of documents known to Applicant in order to comply with Applicant's duty of disclosure pursuant to 37 CFR 1.56. A copy of each listed document is being submitted to comply with the provisions of 37 CFR 1.97 and 1.98.

The submission of any documents herewith, which is not a statutory bar, is not intended as an admission that such document constitutes prior art against the claims of the present application or that such document is considered material to patentability as defined in 37 CFR §1.56(b). Applicant does not waive any rights to take any action which would be appropriate to antedate or otherwise remove as a competent reference any document which is determined to be a prima facie prior art reference against the claims of the present application.

TIMING OF THE DISCLOSURE

The instant Information Disclosure Statement is believed to be filed in accordance with 37 C.F.R. 1.97(b), prior to the mailing date of a first Office Action on the merits (first scenario). If that is not the case, such as in a second scenario in which a first Office Action on the merits has been mailed before the filing of the instant Information Disclosure Statement, then either a certification or fee is required, and a certification is provided below. If neither of the first or second scenarios is the case, such as if a final Office Action or a notice of allowance has been mailed by the PTO (third scenario), then both a certification and fee are required, and in that case a certification is provided below and also the PTO is authorized to obtain the necessary fee to have the instant IDS considered, from Foley & Lardner Deposit Account #19-0741.

CERTIFICATION

The undersigned hereby certifies in accordance with 37 C.F.R. §1.97(e)(1) that items of information A3 – A5 listed on the Form PTO SB/08 submitted with this Information Disclosure Statement were first cited in a communication from a foreign patent office in a counterpart foreign application not more than three (3) months prior to the filing of this Statement. Item of information A1 is a U.S. patent that is a counterpart to item of information A3, and item of information A2 is a U.S. patent that is a counterpart to item of information A5.

RELEVANCE OF EACH DOCUMENT

A translation of a portion of a Japanese Office Action that issued June 9, 2003 with respect to a counterpart Japanese patent application is provided below.

> "A. The inventions as per the following claims of this application could have been easily invented based on the inventions described in the publications indicated below, which had been distributed in Japan or abroad prior to the filing of this application, by a person having ordinary knowledge in the technical field of the invention prior to the filing of this

application, and therefore cannot be patented, as per the stipulations of Article 29, Paragraph 2 of the Patent Law.

B. The inventions as per the following claims of this application are identical to an invention (design) first described in the specification or drawings appended to the patent (utility model registration) application(s) indicated below, which are patent (utility model registration) applications filed earlier than the date of filing of this application and for which a Japanese Examined Patent Application Publication (issuance of a patent gazette or issuance of a utility model gazette) or Japanese Unexamined Patent Application Publication was made after the filing of this application, and the inventor of this application is not the same as the person who made the aforementioned invention (design) as per the patent (utility model registration) application(s) filed prior to the filing of this application, and the applicant of this application at the time of its filing was not the same as the applicant of the aforementioned patent (utility model registration) application(s), and therefore the inventions as per the following claims cannot be patented, as per the stipulations of Article 29-2 of the Patent Law.

Note (For a list of the cited literature, see the List of Cited Literature.)

Reason: A
Claims: 3, 6–8, 11, 14–16, 19, 22–30
Cited Literature: 1

(Remarks)

Cited Literature 1 describes an encryption/decryption device comprising a delay time determination unit that accepts as input random numbers outputted from a random number generator unit and performs determination of delay time of execution delays, which are intentionally inserted during encryption processing/decryption processing, dependently on the random numbers; and a power residue computation means that performs processing on the input data dependently on the delay insertion by said delay time determination unit, and outputs output data that does not depend on the output of said random number generator.

Reason: B
Claims: 1, 2, 4, 5, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18, 20, 21, 23–30
Cited Literature: 2

(Remarks)

The specification or drawings first attached to the application for the filing described in Cited Literature 2 describes an invention for an encryption/decryption device comprising an intermediary data control means that accepts as input random numbers outputted from a random number generator and performs control so as to cancel out the effect of the random numbers by applying multiple random number dependent intermediary data modification operations that change the intermediary data needed during execution of encryption processing/decryption processing dependently on the random numbers; a conditional branching control means that accepts as input random numbers outputted from said random number generator and controls the random number dependent conditional branching decision operations by selecting the procedure to be actually executed from among multiple procedure options dependently on the random numbers; and a computation means that accepts input data as input and, while changing state dependently on the random number dependent intermediary data modification operations of said intermediary data control means and the random number dependent conditional branching decision operations of the conditional branching control means, performs encryption processing/decryption processing on said input data, and outputs output data that does not depend on the random numbers outputted from said random number generator.

Reason: B
Claims: 2, 5, 7, 8, 10, 13, 15, 16, 18, 21, 23–30
Cited Literature: 3

(Remarks)

The specification or drawings first attached to the application for the filing described in Cited Literature 3 describes an invention for an encryption/decryption device comprising a conditional branching control means that accepts as input random numbers outputted from a random number generator, and controls random number dependent conditional branching decision operations whereby the determination of the execution order of encryption procedures/decryption procedures and the selection of the procedure to be actually executed from among multiple

procedure options is carried out dependently on the random numbers; and a computation means that accepts input data as input and, while changing state depending on the random number dependent conditional branching decision operations of said conditional branching control means, performs encryption processing/decryption processing on said input data, and outputs output data that does not depend on the output of said random number generator.

At present , no reasons for rejection have been discovered for inventions as per claims other than the claims indicated in this notice of reasons for rejection. If any reasons for rejection are newly discovered, a Notification of Reasons for Rejection will be issued."

Applicant's statements regarding the Japanese Office Action are based on a partial translation that Applicant's representative obtained. These statements should in no way be considered as an agreement by Applicant with, or an admission of, what is asserted in the Japanese Office Action.

Applicant respectfully requests that the listed documents be considered by the Examiner and formally be made of record in the present application and that an initialed copy of Form PTO SB/08 be returned in accordance with MPEP §609.

Respectfully submitted,

August 14, 2003
Date

Phillip J. Articola
Registration No. 38,819

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5300
Facsimile: (202) 672-5399